Principles of Cryptography Problem Sheet 2

Dr. Kurunandan Jain[1]†,

[1]Department of Mathematics, Amrita Vishwa, Amrita Campus, Kollam-690525, Kerala, India

(Received xx; revised xx; accepted xx)

1) The stream cipher described in chapter 2 can easily be generalised to work in alphabets other than the binary one. For manual encryption, an especially useful one is a stream cipher that operates on letters.

a) Develop a scheme which operates with the letters A, B, $\cdots$ Z, represented by the numbers $0, 1, \cdots 25$. What does the key stream look like? What are the encryption and decryption functions?

b) Decrypt the following cipher text: bsaspp kkuosp which was encrypted using the key: rsidpy dkawoa

2) Assume an OTP-like encryption with a short key of 128 bit. This key is then being used periodically to encrypt large volumes of data. Describe how an attack works that breaks this scheme.

3) We will now analyse a psedorandom umber sequence generated by a LFSR characterized by $c_2 = 1$, $c_1 = 0$, $c_0 = 1$.

a) What is the sequence generated from the initial vector $(1, 0, 0)$

b) What is the sequence generated from the initial vector $(0, 1, 1)$

c) How are the two sequences related?

4) Compute the first two output bytes of the LFSR of degree 8 and the feedback polynomial is $x^8 + x^4 + x^3 + x + 1$

5) Show that $S_1(x_1) \oplus S_1(x_2) \neq S_1(x_1 \oplus x_2)$ for:

a) $x_1 = 000000$ $x_2 = 000001$

b) $x_1 = 111111$ $x_2 = 100000$

c) $x_1 = 101010$ $x_2 = 010101$

6) What is the output of the first round of DES algorithm when the plaintext and the key are both all zeros?

7) Remember that it is desirable for good block ciphers that a change in one input bit affects many output bits, a property that is called diffusion or the avalanche effect. We try now to get a feeling for the avalanche property of DES. we apply an input word that has a 1 bit position 57 and all other bits as well as the key are zero

a) How many S-boxes get different inputs compared to the case when all-zero plaintext is provided?

b) What is the minimum number of output bits of the S-boxes that will change according to the S-box design criteria?

c) What is the output after the first round?

d) How many output bit after the first round have actually changed compared to the case when the plaintext is all zero?

8) Generate the multiplication table for the extension field $GF(2^3)$ for the case that the irreducible polynomial is $P(x) = x^3 + x + 1$. The multiplication table is in this case a 8×8 table.

9) Multiplication in $GF(2^4)$: Compute $A(x) \cdot B(x) \mod P(x)$ in $GF(2^4)$ using the

† Email address for correspondence: kurunandanj@am.amrita.edu

irreducible polynomial $P(x) = x^4 + x + 1$. What is the influence of the choice of then reduction polynomial on the computation?

a) $A(X) = x^2 + 1$ and $B(x) = x^3 + x^2 + 1$

b) $A(X) = x^2 + 1$ and $B(x) = x + 1$